Notes from the NDIA and Army Y2K Workshop

On 14-15 April 1998 the National Defense Industrial Association sponsored an Army Year 2000 Industry Workshop and Exhibition. Their selected theme was, *"Expediting Lessons and Tools for the Final Stretch." These notes represent the various presentations and panel discussions. The slides of LTG Campbell, the DISC4's Keynote will be entered on the Corps' Y2K webpage on April 29, as will be the slides from Mr. Browning's presentation. The other Workshop presentations with slides were to be entered on the DISC4 webpage following the workshop. As of 29 April the slides had not yet been entered on the DISC4 site, which is linked to the Corps website.*

Keynote by LTG Campbell

Discussed the Y2K Home page; the Policy memo is there as are lessons learned.

We must look at the total system and test the total system.

We can only validate Y2K fixes through rigorous testing.

The Army Status and Issues by Miriam Browning, Director for Information Management, DISC4

Mrs. Browning emphasized that Y2K is a management and leadership issue.

However, she said that this is an opportunity to eliminate unnecessary systems.

Commander is responsible for Infrastructure.

The Corps of Engineers has responsibilities for the locks and dams control systems.

For mission critical systems there are only 20 months left.

Certification for all systems that are Y2K compliant.

Panel on *Renovation Tools and Services*, **Harris Miller, ITTA; Michael Higgins, ZMAX; Barry Ingram, EDS; James Olivero, Micro Focus.**

This is a management problem

Risk Assessment: What will get done? What won't?

Conversion is estimated to cost $1.50 per line.

All interface systems must comply.

Here are the things they said you need:

Awareness
Education
Commitment [**Need Top Management**]
Well Defined Plan
Someone in Charge
Motivation
Sense of Urgency

Information sharing is critical.
Need certification program both vendors and end users.

Management should know status at all times.

Vendors - understand deliverables - costs
be creative in retaining people
No viruses can be introduced.
Cost will be higher than we think.
Need to establish a testing discipline.

Mission Critical Systems are FIRST.
Tools are not magic.
Plan
Manage
START
Audit through every phase of the "fix."
WINDOWING: Code only where there are calculations, which it is estimated

Find the Program
Find the Dates
Fix the dates
and TEST, TEST..would be about 1 line in 823.

Testing and Validation, a panel, **Robert Martin, MITRE Corp.; Madav Panwar, GAO; Keihan Sedghi, Mantech; and Hoyt Warren, CACA.**

Test only in a test environment and make sure the test environment is Y2K Complaint.

With automated testing tools, users will require training.

There are many available, choose the best for your job.

Invite vendors to demonstrate tools in your environment.

You need testing expertise.

They plan to have a draft testing guide on the webpage by June.

Contingency plans must cover what happens if a system doesn't work.

William Curtis, DOD Y2K Project Manager [new only in job 4 weeks]

Plans to have guidance out on a final game plan by May.

They plan to establish 42 Interface Assessment Workshops for functional proponents to be held between now and Sep 98.

They are looking at a Y2K Certification Force; 250 five person teams to go around checking Certifications.

They are also looking at setting up an Emergency Reaction Force.

There is a critical shortage of skilled personnel.

A panel, *Contingency Planning and Risk Mitigation.* Panelists: **Judith Draper**, ***CSC; Ken Owen, Tava Technologies; Julia McCreay-Laws, IRS; and Noel Goyette, CSC.***

TRIAGE: Systems that can survive on their own
Systems that can survive with help
Systems that won't survive

Focus on critical mission systems only. That's all the time we have left.

Y2K potential problems are global.

We have a poor reputation for bringing in systems on time and on budget.

Those systems that won't make it need contingency plans.

Get support from internal audit.

Be honest, this is a time for candor.

With embedded systems there is little or no documentation. There has not been any IT involvement in the development and these will not be easily tested

Vendors are afraid of litigation.

In looking at contingency plans and risk assessment minimize the scope and take a TRIAGE view.

Risk Assessment must be done by functional proponents

Panel on *Legal Issues,* **by Helaine Elderkin, Esq Army Science Board; Douglas DeMoss, Esq USA; Clarence Long, Esq, USAF; and James Hughes, Jr., Esq, Patton, Boggs, LLP.**

Who must pay to fix old system? What can we do to assure new system comply?

With Embedded IT if it is not specified in the product, the contractor may be liable.

Be sure to check out and test any new system before acceptance. Withholding acceptance is the strongest penalty we have.

Assure a Y2K clause in every contract to assure that it meets the requirements of Y2K.

“The Warranty Provision” may be a good incentive to contractors and vendors.

Be sure that Y2K is stated in the SOW.

Know the terms of your contract. Focus on the work to be done. Define the test procedures and criteria for acceptance.

Assign responsibility for data conversion.

Be sure to define existing interfaces and new interfaces.

Always include the Y2K clause.

Cooperate with private systems and vendors.

Do not certify falsely. CHECK WITH YOUR COUNSEL about certification.

A Panel, *Lessons Learned,* panelists were: **Col Richard Johnson, PEO STAMIS; Col Kevin Greaney, Cdr, SDC-W; LTC (P) Bruce Bachus,**

ODCSPER IMO; Maj Dana Barrett, TRADOC DCSIM; William Dates, DISC4.

You must know your interfaces and think networks.

Prioritize critical systems.

Remember, even when we have delivered systems, we've had bugs.

The Y2K is more a management issue than technical. We need plans, schedules, resources based on our inventories and risk assessments.

Remember risk management is continuous.

Functional proponents are essential for contingency plans

Control systems outside our control with "firewalls."

Systems interface agreements must be closely monitored. What are they doing, when, how, etc.

DON'T assume compliance - TEST, TEST [look fore date dependent utilities]

See any vendor's test plan and results.

The perfect testing tool does not exist.

They now have multi-language testing tools, configuration management and tracking tools.

Look at lease rather than purchase.

Test early, leave time to fix. Have a good test plan with exit criteria.

Be sure your system test includes interfaces.

Automated testing tools can lower the time involved.

Be sure to involve Senior Management.

Concentrate on the most important systems; and assure that concentration is on the total system, infrastructure and interfaces

Commit resources at HQ and program levels.

Don’t take anything for granted.

Y2K is a leadership problem. Involve leadership in planning, testing, etc. Keep them informed and involved.

System interface agreement is a must for testing.

Plan for functional resistance. Decide on acceptable level of risk and plan accordingly.

Make sure your COTS is Y2K complaint. Test is the only way to determine if it is good enough.

Army Y2K Industry Workshop

LTG William H. Campbell

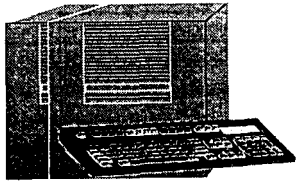
Director of Information Systems
for Command, Control,
Communications and Computers

Arlington, VA
14 April 1998

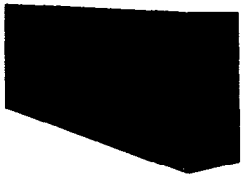
OUTLINE

- **Army Y2K policy**
- **Lessons learned**
- **Government and industry together**
- **The final stretch**

Scope and Cost of Y2K Problem in the Army*



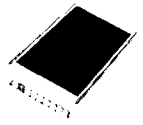
Army Information Systems
$115M



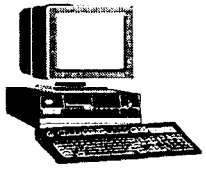
MACOM/Installation Unique Systems
$41M

Weapon Systems
$39M

12,240 Weapon & Automation Systems have Y2K problem - $195M is cost to fix



Communications Hardware/Software
$72M



PC's & Servers
$91M

Facilities/Infrastructure
$8M

196,802 Infrastructure devices have Y2K problem - $171M is cost to fix

Systems Requiring Repair

•Major Mission Critical Systems	120
•Other Major Systems	119
•Non - Major Systems	12,001
•Total	12,240

Bottom Line
Systems & devices to be fixed: 209,042
Total cost estimate: $366M

*January 1998

ARMY YEAR 2000 POLICY *

- Fixing **Y2K** is a "MUST SUCCEED" mission
- **Y2K** fixes must be made before all nonessential and sustainment and enhancement requirements are accomplished
- No new funding
- Opportunity to eliminate unnecessary systems

*Secretary of the Army and Chief of Staff of the Army Memo, subject: Year 2000 Fixes--Top Priority, 3 1 March 1997

ARMY YEAR 2000 POLICY *

- Certification - by 1 April 1998 provide certification for all systems in the Army

- Contingency planning - by 1 June 1998 completed contingency plans for all systems in the Army y2K database that are not Y2K compliant

- Interface agreements (new OMB requirement) - systems owners must inventory all data interfaces by 1 February 1998 and coordinate with interfacing partners by 1 March 1998

*Updated policy memo - 9 February 1998, subject: Fixing Year 2000 Issues

ARMY YEAR 2000 MANAGEMENT STRATEGY

- **Goal:** ensure no critical system failures occur due to Y2K related problems
- **Approach:** centralized management - decentralized execution
- **Five Phased Action Plan**
  - **Awareness (31 Dec 1995 - 31 Dec 1996)**
  - **Assessment (31 Mar 1996 - 31 Mar 1997)**
  - **Renovation (31 Dec 1996 - 30 Sep 1998)**
  - **Validation (31 Mar 1997 - 31 Dec 1998)**
  - **Implementation (30 Jun 1997 - 31 Dec 1998)**
- **Resourcing:**
  - OMB/DoD/Army Guidance: Use existing resources to fix Y2K problems
- **Primary Management Tools:** US Army Y2K Management Plan, US Army Year 2000 Database (USAY2KDB), AAA, DAIG, IPRs

LESSONS LEARNED

- Share Results
  - Web pages
  - OSD Interface Assessments
  - Best Tool Set (Right Tool for the Right Job!)
  - Testing, Validation and certification
    - Tactical Systems
    - Sustainment Base Systems
    - Cross Functional Systems Testing
- Partner/Work with Industry
  - Use Industry Best Practices
  - Share Results/Lessons Learned

Things to Check

- Must Evaluate Total Systems -- Hardware, Software, Databases -- Some Peripheral Devices Like Uninterruptible Power Supplies Have Embedded “Clocks”
- Must Assume Hidden Y2K Problems Exist
- Must Anticipate “Regression” to Earlier Phases in Complex Systems As Y2K Fixes Are Tested
- Must Include Support Equipment in Weapon System Assessment and Renovation Efforts.
- Need Emergency Response Capability and Contingency Plans

Things To Check (cont.)

- Ensure all interface agreements (MOUs) have been completed and that all interfaces are and during testing.
- Certification assessments must be based upon supporting evidence.
- Must validate Y2K fixes through rigorous testing-- When You believe it's compliant, roll the clock forward and run a"Safety Certification"
- Common Processor related Y2K Problems
  - The processors are compliant, but motherboard's Basic Input Output System (BIOS) chips are not.
  - Older BIOS Chips cannot be reprogrammed
  - BIOS problems also exist in older modems and video cards
  - "RightTime" only works on AT class machines, running DOS 3.x or better
  - Newer versions of IBM and Microsoft Disk Operating System (DOS) are compliant however, their utilities are not (FDISK, FORMAT, etc.)

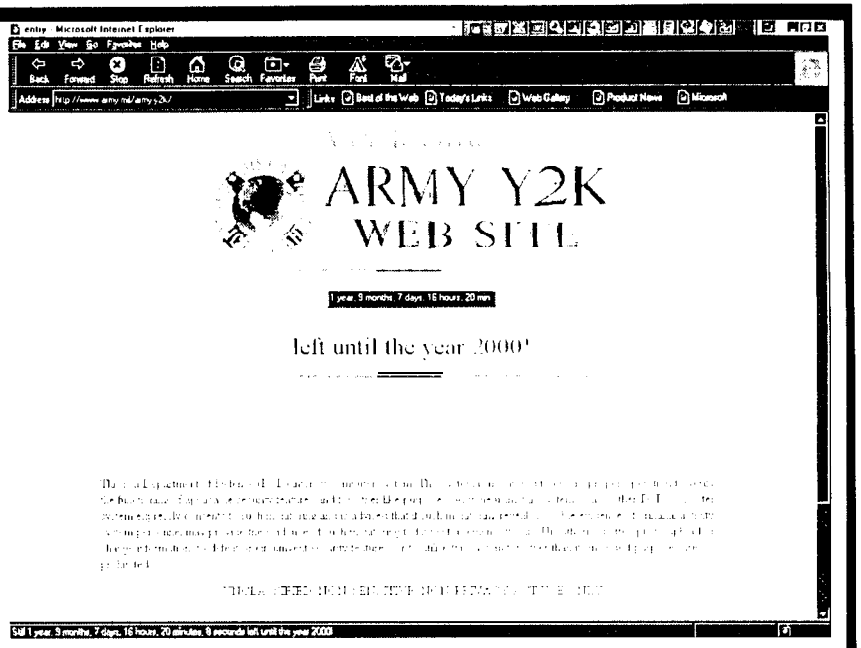
GOVERNMENT AND INDUSTRY TOGETHER

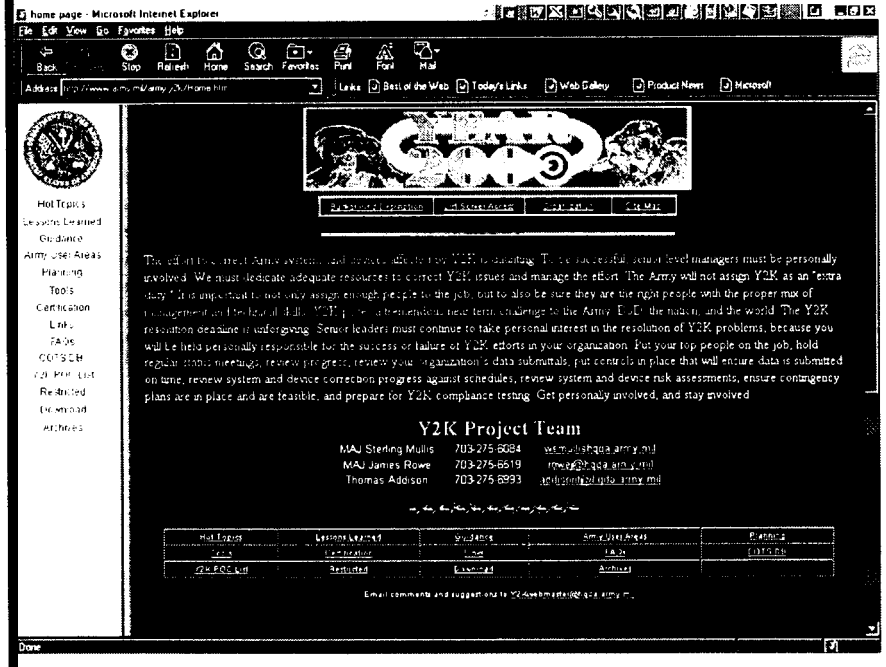
- Renovation - Tools and Services
- GAO findings
- Testing and Validation
- Contingency Planning and Risk Mitigation
- Legal Issues
- Defense Science board findings
- Army Lessons Learned

Sources of Help

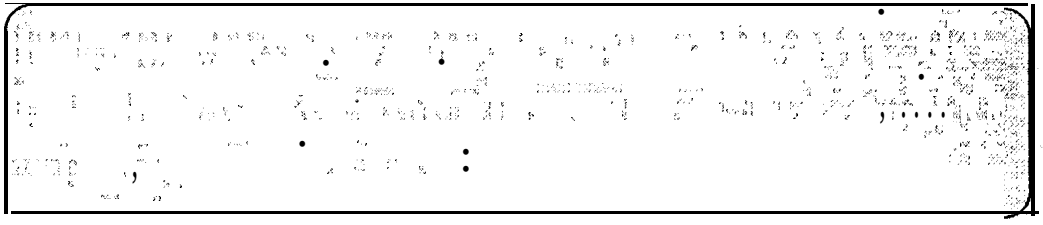
Wealth of Knowledge On Line

- Compliance Checklist
- Risk Management, Contingency, & Test Templates
- Tools Catalog
- Up to Date Guidance & Lessons Learned
- COTS Hardware/Software Quick-Look Assessments





- Army Consolidated Enterprise Services(ACES) GSA Blanket Purchase Agreement(BPA) awarded to CSC, EDS, IBM, and UNISYS
  - Provides contract services for outsourcing, business process reengineering, information security, and Year 2000
  - POC is Stephen Timchak, (703) 325- 17 19, DSN 211-1719

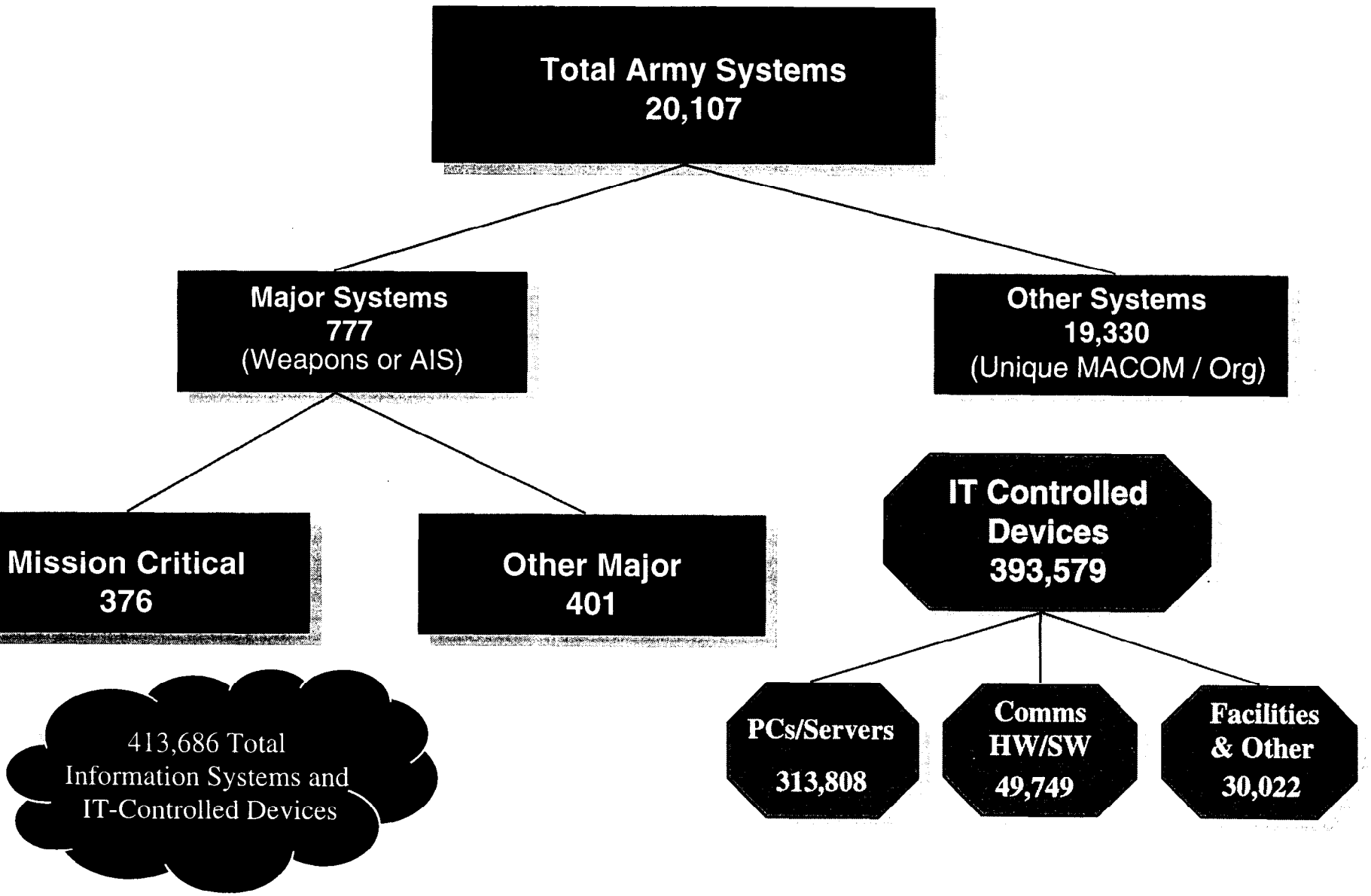


Back up

Things To Check (cont.)

- Other Potential Weapons System Problems:
  - Date Displays to Operators (non-compliant)
  - Uses date information to determine location of satellites for navigation (questionable)
  - Support/diagnostic equipment to maintain operations (questionable)
  - Currently uses Computer Electronics Units (CEUs), Central Processing Units (CPUs), Power Control Units (PCUs), with embedded chips for systems operations. (must check out)
  - Interfaces with Mobile Subscriber Equipment (need MOA)
  - Interfaces with GPS for Navigation (validate)
  - Reliance on External Timing Source

ARMY SYSTEMS BREAKOUT



THEFINALSTRETCH

- Importance of first hand testing
- Interoperability between systems
- Inspecting to insure results

THE YEAR 2000
Ensuring the Army Will Be Ready

ARMY STATUS, ISSUES, AND ASSISTANCE

Miriam F. Browning

Director for Information Management

HQDA - ODISC4

Brownmf2@ hqda.army.mil

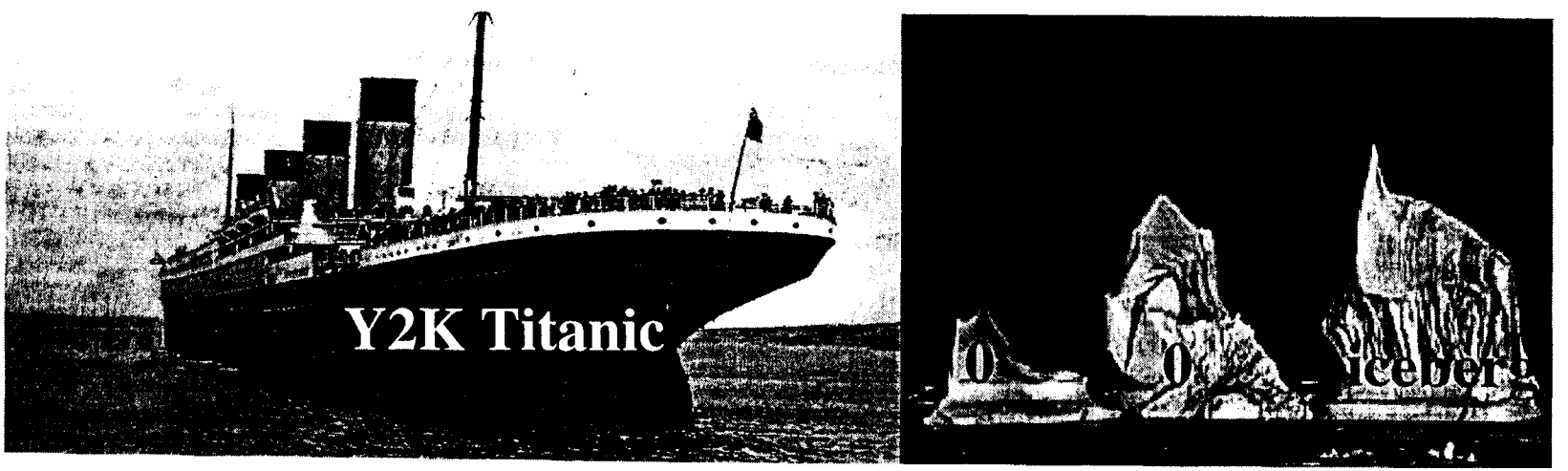
703-695-5489

Army Y2K Overview

- Dilemma
- Current Status
- Issues
- Assistance and Tools
- Summary

PRESENT DILEMMA

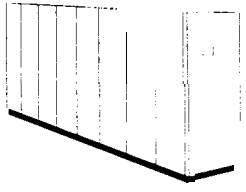
Will the Y2K Titanic crash into the iceberg of the next millennium or sail by harmlessly?



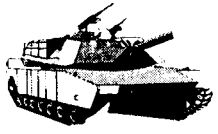
Army leadership, systems owners/developers, and contractors are the captains of this ship.

Scope and Cost of Y2K Problem in the Army*

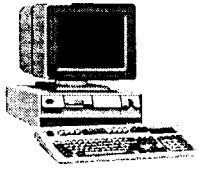
Army Information Systems $115M



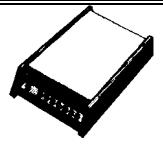
MACOM/Installation Unique Systems $41M



Weapon Systems $39M



PC's & Servers $91M



Communications Hardware/Software $72M

Facilities/Infrastructure $8M

12,240 Weapon & Automation Systems have Y2K problem - $195M is cost to fix

196,802 Infrastructure devices have Y2K problem - $171M is cost to fix

Bottom Line
Systems & devices to be fixed:
209,042
Total cost estimate: $366M

Systems Requiring Repair

• Major Mission Critical Systems	120
• Other Major Systems	119
•Non - Major Systems	12,001
*Total	12,240

*January 1998

ARMY Y2K MANAGEMENT STRATEGY

How do we ensure 100% of our systems are either fixed or retired?

- **Establish Responsibility**
  - Army Acquisition Executive (AAE) policy memo - March 1996
  - US Army Y2K Management Plan - October 1996
  - Secretary of the Army/Chief of Staff Army (SA/CSA) Memo - March 1997
  - CIO policy on interfaces, contingency plans, and certification - Feb 1998
- **Track Progress**
  - Y2K database and quarterly reports - ongoing
  - Army Audit Agency readiness assessments - ongoing
  - Army Y2K progress reviews - August 1997 and ongoing
- **Provide Information and Tools**
  - Senior level awareness program
  - Army Y2K web sites
  - Army Y2K contracts

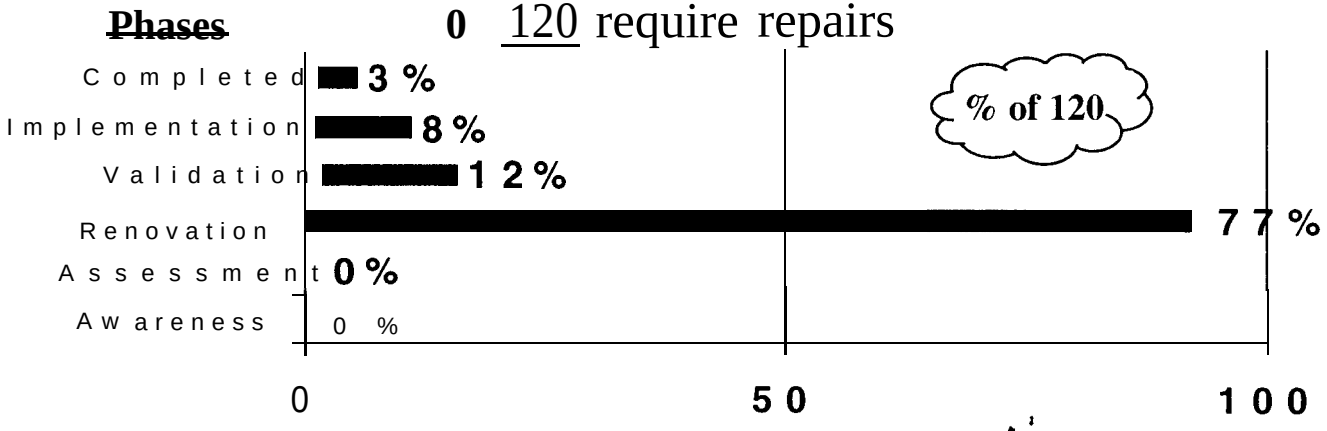
ARMY YEAR 2000 POLICY*

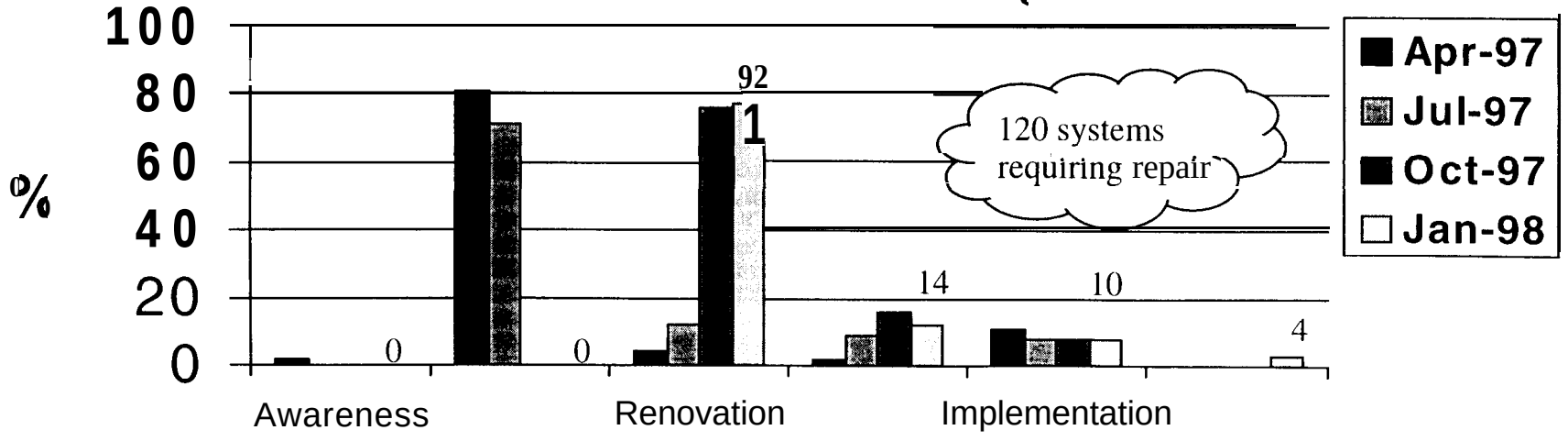
- Fixing Y2K is important for the Army warfighting mission and Army credibility with the American public
- Y2K fixes must be made before all nonessential sustainment and enhancement requirements are accomplished
- ☠□ new funding
- Opportunity to eliminate unnecessary systems

*Secretary of the Army and Chief of Staff of the Army Memo, subject: Year 2000 Fixes--Top Priority, 31 March 1997

PROGRESS - MISSION CRITIC AL SYSTEMS
CURRENT STATUS AND TRENDS

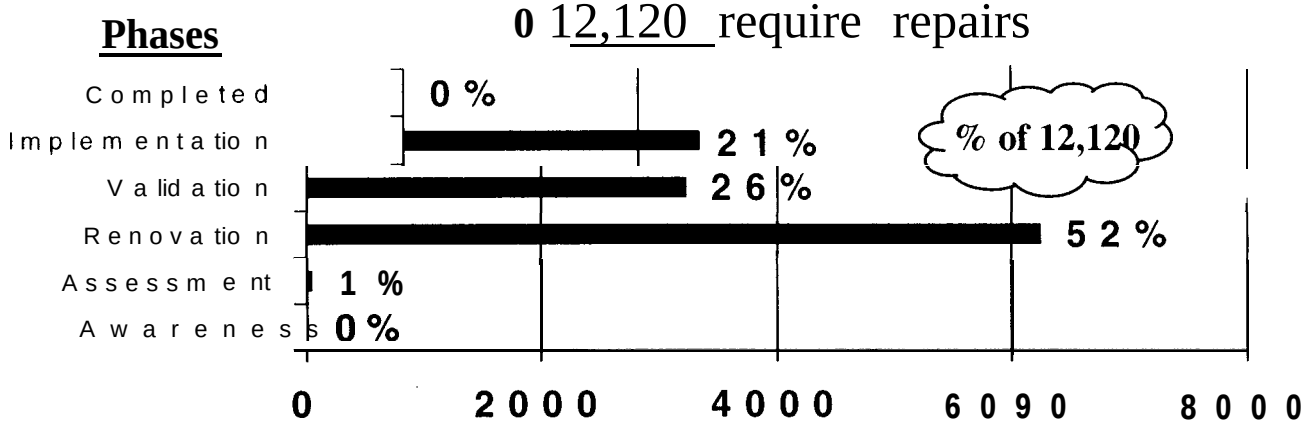
- **376 Mission Critical** Systems
  - o 160 are compliant
  - o 96 will be retired or replaced
  - 0 120 require repairs

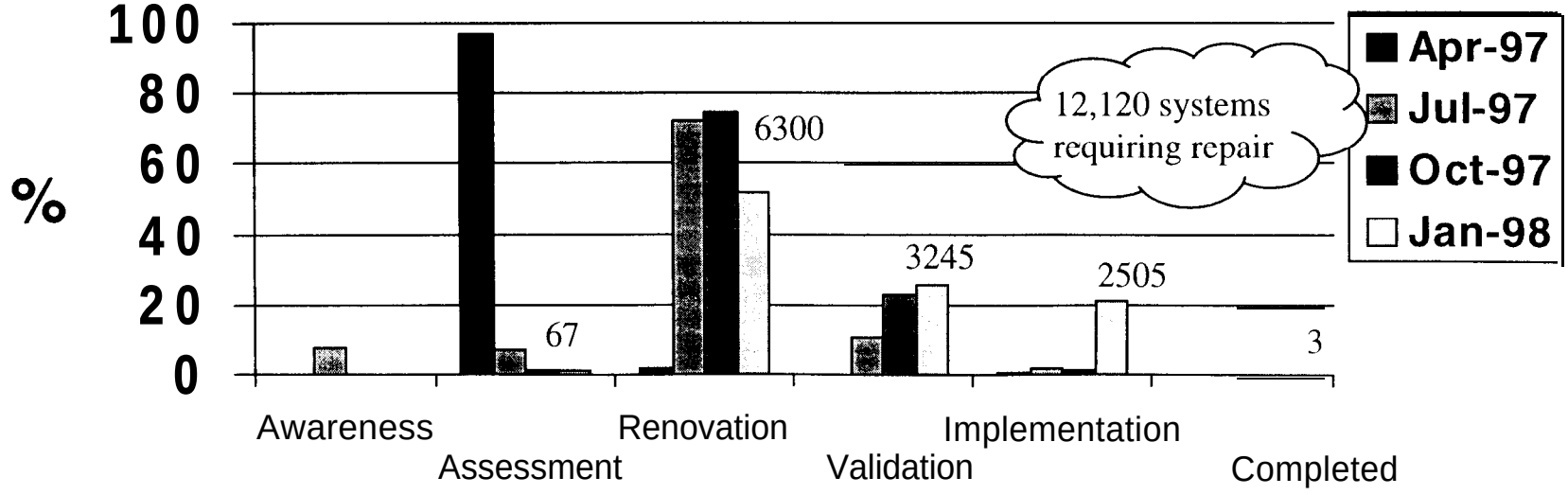




PROGRESS - NON-MISSION CRITICAL SYSTEMS CURRENT STATUS AND TRENDS

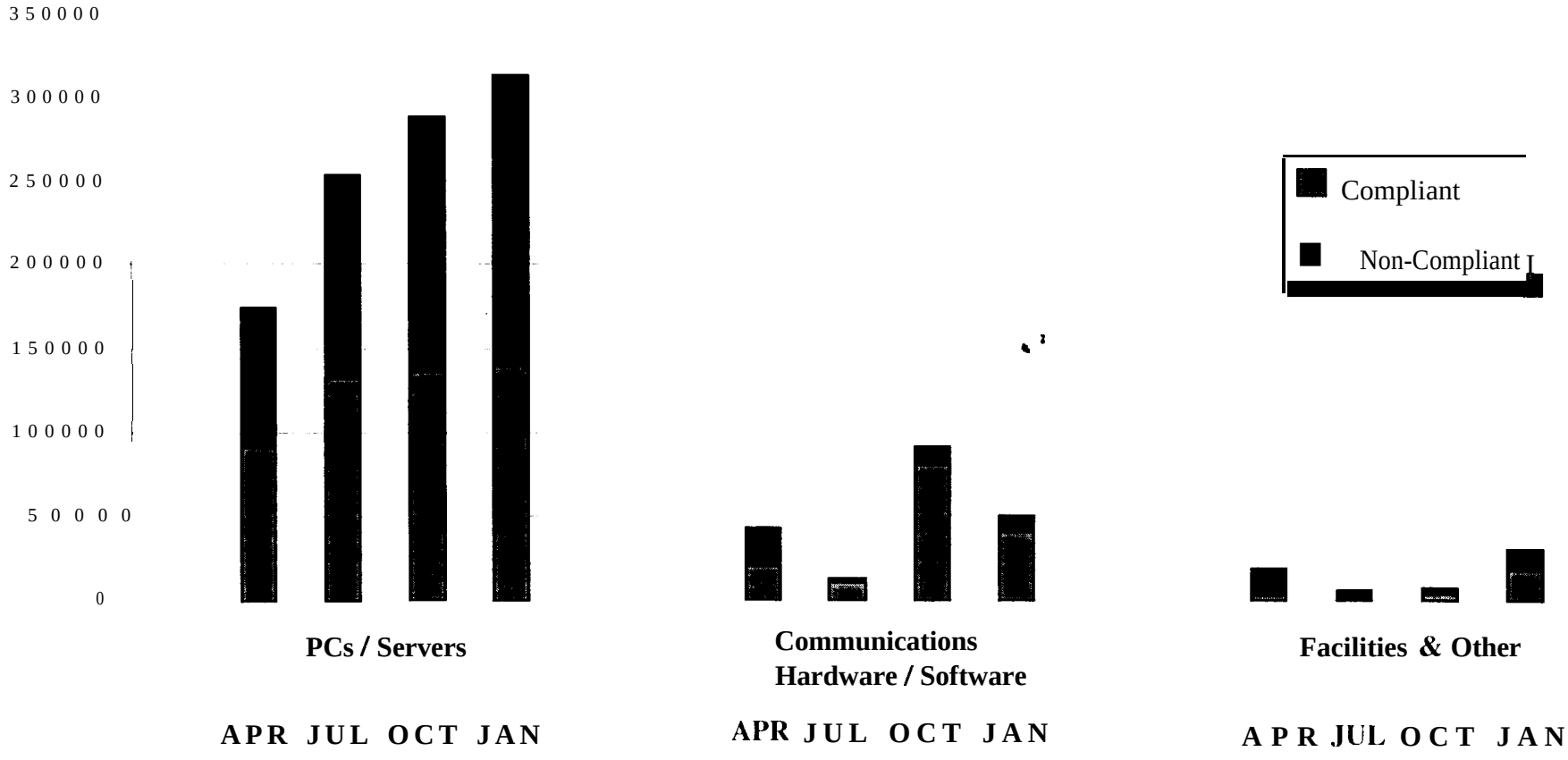
- 19,731 **Non-Mission Critical** Systems
  - o 6,699 are compliant
  - o 9 12 will be retired or replaced
  - 0 12,120 require repairs





PROGRESS - INFRASTRUCTURE CURRENT STATUS AND TRENDS

- 393,579 Total IT-Controlled Devices
  - 196,777 are compliant
  - 196,802 are non-compliant



ISSUES

1. Resources

Dollars - No new money

- Commanders must resource Y2K from existing funds, assuring Y2K fixes are a top priority
- Non-essential enhancements must be deferred until Y2K problems are resolved
- Opportunity to eliminate unnecessary systems

People - two incentives available

- Waiver of dual compensation reductions for retired military officers and re-employed civilian annuitants
- Use of premium pay to attract and retain employees in emergency situations

ISSUES

2. Infrastructure
   - Commanders responsible for all Y2K areas on an installation - a priority review item
   - Centrally managed systems are being addressed by appropriate Army PMs
   - Corps of Engineers is placing priority attention on control systems for locks and dams

3. Contingency Plans
   - Required by 1 June 1998 for all Y2K non-compliant systems
   - Responsibility of systems owners and commanders

ISSUES

4. Testing
   - Dollars and test plans should be in place
   - Infrastructure for testing software should be Y2K compliant
   - Major interfaces and players need to be considered

5. Compliance Considerations
   - Certification documents necessary for all Y2K compliant systems
   - DoD considering the use of certification teams

ASSISTANCE

- Army Audit Agency
  - Will perform "Y2K readiness assessments" for commands, PEOs/PMs, HQDA functional proponents

- OSD Y2K Interface Assessment Workshops
  - Over 48 planned between now and Sep 1998, covering over 21 different DoD functional areas

- Army Consolidated Enterprise Services (ACES) GSA Blanket Purchase Agreement (BPA) awarded to CSC, EDS, IBM, and UNISYS
  - Provides contract services for outsourcing, business process reengineering, information security, and Year 2000
  - POC is Stephen Timchak, (703) 325-l 719, DSN 211-I 719

TOOLS

- Army Y2K Website (http://www.army.mil/army-y2k)
  - Tools and lessons learned
  - Commercial products status
  - Policy and guidance
  - Links to other websites, govt and commercial
- Assistant Chief of Staff for Installation Management website (http://www.hqda.army.mil/acsimweb/ops/y2k.htm)
  - Facilities infrastructure devices, e.g., HVACs, Intrusion Detection Systems
  - Infrastructure checklists
- Army Y2K Data Base
  - Web-enabled to capture and transmit Army data to OSD, OMB, and Congress

SUMMARY

- Y2K is a major Army readiness issue
- Fixing Y2K is the responsibility of senior leaders, systems owners/developers, and contractors
- Highest priority is assuring all mission critical systems are fixed on schedule and are certified
- Much work to be done on renovation, testing, contingency planning, and certification

Y2K is Everyone's Business!